Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously presented): An electronic authentication method comprising:

in a first information processing apparatus, receiving a request for contents from a second information processing apparatus;

in response to said request, generating an ~~identifier~~ encryption key and an access number that ~~is~~ are associated with said requested contents ~~in a first information processing apparatus~~;

producing enhanced content comprising said requested contents, said encryption key, and said access number;

~~combining said contents and said identifier to produce enhanced content;~~

transmitting said enhanced content to ~~a~~ said second information processing apparatus;

presenting said enhanced content to a user at said second information processing apparatus~~, said identifier being combined with said contents in a manner that it is visually imperceptible to said user~~;

in said second information processing apparatus, accessing said encryption key and said access number from said enhanced content;

receiving user data in said second information processing apparatus and in response thereto producing input data from said user data~~, including obtaining said identifier from said enhanced contents~~, wherein at least some of said input data is encrypted with said encryption key, said ~~produced based on said identifier~~; and

transmitting said input data from said second information apparatus to said first information apparatus as received input data[.],

wherein said first information processing apparatus can authenticate legitimacy of said received input data based on said access number.

2-3. (Canceled)

4. (Currently amended): An electronic authentication method according to claim ~~3~~1, wherein: said embedded encryption key is a public key; said received input data is decrypted using a private key associated with said public key; and said public key and said private key are generated in said first information processing apparatus.

5. (Currently amended): An information processing method comprising:

generating an encryption key and an access number that are associated with ~~identifier for~~ contents;

creating an access information record corresponding to said encryption key and said access number;

~~storing said identifier as a stored identifier;~~

~~generating a second identifier;~~

incorporating said ~~identifier~~ encryption key and said access number into ~~second identifier with~~ said contents to produce enhanced contents ~~such that when said enhanced contents is displayed to a user, said identifier and said second identifier are visually imperceptible~~;

transmitting said enhanced contents to an external apparatus;

receiving received data from said external apparatus, said received data including a user-provided access number, at least a portion of said received data being encrypted with said encryption key;

decrypting said received data; and

deleting said access information record based on whether said received data could be decrypted and based on a comparison with said access number and said user-provided access number.

~~acquiring an acquired identifier for said contents; and~~

~~carrying out processing based on said received data and invalidating said stored identifier if said acquired identifier matches said stored identifier.~~

6-7. (Canceled)

8. (Previously presented): An electronic authentication system comprising a first information processing apparatus and a second information processing apparatus wherein:

said first information processing apparatus comprises:

a means for generating an ~~identifier for~~ encryption key and an access number associated with first contents;

a storage means for storing a record that corresponds to said encryption key and said access number~~at least a first portion of said identifier as a stored identifier~~; and

a means for transmitting enhanced contents ~~and said identifier~~ to said second information processing apparatus, ~~including embedding means for embedding said identifier in said contents to produce~~ said enhanced contents comprising said first contents, said encryption key, and said access number;

said second information processing apparatus comprises:

a means for inputting user data, including means for displaying received enhanced contents~~such that said identifier is not visually perceivable by a user~~; and

a means for transmitting said user data and said identifier to said first information processing apparatus as input data, wherein said input data is generated by ~~processing~~ encrypting said user data and includes said access number~~said first portion of said identifier based on a second portion of said identifier~~; and

there is further provided in said first information processing apparatus a processing means for authenticating legitimacy of said input data received by said first information processing apparatus and deleting said record based at least on a comparison of said access number and said access number contained in said received input data~~invalidating said stored identifier if said first portion of said identifier contained in said input data matches said stored identifier~~.

9. (Previously presented): An electronic authentication system according to claim 8, wherein said second information processing apparatus further comprises an acquirement

means for acquiring said ~~identifier~~ encryption key and said access number from said received enhanced contents.

10. (Previously presented): An electronic authentication system according to claim 8, wherein said second portion of said identifier is an encryption key; and said first information processing apparatus further comprises a reception means for receiving an identifier encrypted by using said encryption key and decrypting said encrypted identifier.

11. (Currently amended): An information processing apparatus comprising:

a generation means for generating an identifier for contents, said identifier comprising and encryption key and an access number ~~a first part and a second part~~;

a storage means for storing at least said first part of said identifier as a stored identifier;

a transmission means for transmitting enhanced content comprising said contents and said identifier to an external apparatus ~~as enhanced contents, wherein said enhanced contents comprises said identifier embedded in said contents such that upon displaying said enhanced contents to a user, said identifier is substantially visually imperceptible~~;

a reception means for receiving received data from said external apparatus, said received data comprising a user-provided access number and a portion that has been encrypted using said encryption key;

an acquirement means for acquiring ~~an acquired identifier~~said user-provided access number from said received data; and

a processing means for ~~carrying out processing based on said received data and invalidating~~deleting said stored identifier if said ~~acquired identifier~~user-provided access number matches said ~~stored identifier~~access number.

12. (Canceled)

13. (Currently amended): An information processing apparatus according to claim 11, wherein ~~second portion of said identifier is an encryption key; and~~ there is further

provided a reception means for ~~receiving an identifier encrypted by using said encryption key and~~ decrypting said portion of said received data that has been encrypted ~~encrypted identifier~~.

14. (Currently amended): An information processing apparatus comprising:

a contents requesting means for requesting an external information processing apparatus to transmit contents;

a reception means for receiving said requested contents, an identifier comprising an encryption key and an access number being embedded in said requested contents;

a display means for displaying said requested contents to a user~~, wherein said identifier is substantially visually imperceptible~~;

an extraction means for extracting said identifier from said requested contents;

an input means for inputting user data from a user; and

a transmission means for transmitting, as secured data, said user data and ~~a first portion of said identifier~~said access number to said external information processing apparatus, at least a portion of said secured data being encrypted by said encryption key~~generated using a second portion of said identifier~~.

15. (Canceled)

16. (Currently amended): A storage medium for storing information readable by a computer, said medium characterized in that said information includes:

a generation function for generating an ~~identifier~~ encryption key and an access number for first contents;

a storage function for storing a ~~first~~ stored identifier corresponding to said encryption key and said access number~~portion of said generated identifier~~;

a transmission function for transmitting said contents ~~and~~, said identifier, and said access number to an external apparatus as enhanced content~~, wherein said generated identifier is embedded in said contents such that upon displaying said enhanced contents to a user, said generated identifier is substantially visually imperceptible~~;

a reception function for receiving received data from said external apparatus, said received data comprising a user-provided access number and a portion that is encrypted using said encryption key;

an acquirement function for acquiring ~~an identifier for said contents~~ said user-provided access number from said received data; and

a processing function for authenticating legitimacy of said received data and invalidating said stored identifier if said ~~acquired identifier~~user-provided access number matches said ~~stored identifier~~access number.

17. (Canceled)

18. (Currently amended): A storage medium for storing information readable by a computer according to claim 16, wherein ~~said generated identifier includes a second portion that is an encryption key; and~~ said information further includes a function for ~~receiving said data encrypted by using said encryption key and~~ decrypting said received ~~encrypted~~ data.

19. (Currently amended): A storage medium for storing information readable by a computer, said medium characterized in that said information includes:

a contents requesting function for requesting an external information processing apparatus to transmit contents;

a reception function for receiving said requested contents, an identifier being embedded in said contents, said identifier comprising an encryption key and an access number;

a display function for displaying said requested contents to a user~~, wherein said identifier is substantially visually imperceptible~~;

an extraction function for extracting said identifier from said contents;

an input function for inputting user data from a user; and

a transmission function for transmitting, as input data, said user data and ~~a first portion of said identifier~~said access number to said external information processing apparatus, a portion of said input data being encrypted using said encryption key~~generated using a second portion of said identifier~~.

20. (Currently amended): A storage medium for storing information readable by a computer according to claim 19, wherein ~~said second portion of said identifier is an encryption key,~~ said medium characterized in that said information further includes a function for encrypting said user data by using said encryption key.

21. (Currently amended): An electronic authentication method comprising:

generating an identifier for contents in a first information processing apparatus, said identifier comprising an encryption key and an access number;

driving said first information processing apparatus to store at least a first portion of said identifier and the present time as a storage time in a storage unit;

transmitting said contents and said identifier to a second information processing apparatus as enhanced content, wherein said identifier is embedded in said contents;

presenting said enhanced content to a user at said second information processing apparatus~~, said identifier being visually imperceptible to said user~~;

inputting user data ~~from a user received by said second information processing apparatus~~ in said second information processing apparatus;

transmitting, as secured data, said user data and said ~~first portion of said identifier~~access number contained in said enhanced content from said second information processing apparatus to said first information processing apparatus, a portion of said secured data encrypted by said encryption key contained in said enhanced content~~generated based on a second portion of said identifier~~; and

invalidating said first portion of said identifier stored in said storage unit if said identifier received by said first information processing apparatus is not stored in said storage unit or a time of a predetermined length has lapsed since said storage time stored in said storage unit.

22. (Currently amended): An electronic authentication method, comprising:

generating an encryption key and an access number that ~~is~~ are associated with contents in a first information processing apparatus;

embedding said encryption key and said access number into said contents to produce enhanced content ~~such that when said enhanced content is displayed to a user said encryption key is substantially imperceptible~~;

transmitting said enhanced content to a second information processing apparatus;

displaying said enhanced content in said second information processing apparatus;

inputting user data ~~from a user that has been received by said second information processing apparatus~~ in said second information processing apparatus;

obtaining said access number from said enhanced data;

encrypting said user data using said encryption key to produce secured input data, including acquiring said encryption key from said enhanced content;

transmitting said secured input data and said access number from said second information processing apparatus to said first information processing apparatus; and

validating said secured input data based on said access number and by decrypting said secured input data with a decryption key.

23. (Canceled)

24. (Currently amended): An authentication method in a system in which a first computer making a request for a service is connected to a second computer rendering services via a network, requested contents being transmitted from the second computer to the first computer, data being transmitted from the first computer to the second computer associated with the contents, said method comprising:

generating at the second computer an encryption key relating to the contents;

generating at the second computer an access number for accessing the contents and cataloging the access number in a storage unit;

embedding the encryption key and the access number in the contents to produce enhanced content ~~so that the access number is substantially visually imperceptible when the enhanced content is displayed~~ and transmitting the enhanced content to the first computer;

displaying the contents at the first computer;

generating secured data at the first computer by processing user-provided data with the access number fetched from the enhanced content and transmitting the secured data to the second computer, some of the secured data being encrypted with the encryption key fetched from the enhanced content; and

at the second computer authenticating validity of the secured data based on the access number in the secured data and by decrypting the secured data ~~received at the second computer~~ with a decryption key.

25. (Previously presented): An authentication method according to claim 24, wherein the encryption key is a public key and the decryption key is a private key.

26 - 34. (Canceled)